AFFIDAVIT IN SUPPORT OF A SEARCH WARRANT

I, Nathan A. Cravatta, being duly sworn, hereby state as follows:

INTRODUCTION

1. I am a Special Agent with the Department of Homeland Security, Homeland Security Investigations (HSI), an investigative branch of the United States Department of Homeland Security. I am a federal law enforcement officer authorized by the Secretary of Homeland Security to request the issuance of criminal complaints and search warrants. As a federal agent, I am authorized to investigate violations of laws of the United States and to execute warrants issued under the authority of the United States. I have been employed as a Special Agent with HSI since May 2005. I am currently assigned to the Resident Agent in Charge Office in Milwaukee, Wisconsin.

2. My experience as an HSI agent has included the investigation of cases involving the use of computers and the Internet to commit violations of federal law involving child exploitation, including the production, transportation, receipt, distribution and possession of child pornography. I have received training and have gained experience in interviewing and interrogation techniques, arrest procedures, search warrant applications and the execution of searches and seizures involving computer crimes. I have investigated and assisted in the investigation of criminal matters involving the sexual exploitation of children which constituted violations of Title 18, United States Code, Sections 2251, 2252 and 2252A.

3. I am responsible for investigating violations of federal laws, including the offenses of advertisement, production, transportation, receipt, distribution, and possession of child pornography (as defined in Title 18, United States Code Section 2256) in interstate or foreign commerce by any means, including by computer.

4. The statements contained within this affidavit are based on my training and experience as well as the training and experience of and information communicated to me by other law enforcement personnel with whom I have personally spoken or communicated via email.

5. This affidavit is made in support of an application for warrants to search: (1) the entire premises located at 5412 S. Hately Avenue, Cudahy, Wisconsin ("SUBJECT PREMISES"), more particularly described as a single story residence, with light brown brick on four sides, and dark brown wood trim covering a majority of the front of the residence. The residence has a front porch area with brown pillars, and the window trim is tan. There is an attached one car garage on the south side of the residence. The outer front door is brown. The numbers "5412" are gold colored and are to the right of the front door entrance. The residence is on the east side of the street, and is the second residence south of East Mallory Avenue; (2) a vehicle registered to the target of this investigation ("SUBJECT VEHICLE"), a blue 2017 Chevrolet Silverado truck bearing Wisconsin license plate number MP8182, that is registered to Brett Bedusek at the SUBJECT PREMISES; and (3) the person of Brett Bedusek ("SUBJECT PERSON"), in order to seize and search any electronic devices or media in his possession.

6. Because this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only those facts that I believe are necessary to establish probable cause to believe that evidence, contraband, fruits and instrumentalities of violations of Title 18, United States Code, Sections 2251, 2252 and 2252A, incorporated herein by reference as if fully set forth, are located in and at each of the locations for which authority is requested to search. Where statements of others are set forth in this affidavit, they are set forth in substance and in part.

7. The purpose of this application is to seize evidence of violations of 18 U.S.C. §§ 2252(a)(4)(B) and 2252A(a)(5)(B), which make it a crime to possess child pornography; violations of 18 U.S.C. §§ 2252(a)(2) and 2252A(a)(2), which make it a crime to distribute or receive child pornography in interstate commerce by computer; 18 U.S.C. §§ 2252(a)(1) and 2252A(a)(1), which make it a crime to transport or ship child pornography in interstate commerce; 18 U.S.C. § 2252A(g), which makes it a crime to engage in a child exploitation enterprise; and 18 U.S.C. § 2251, which makes it a crime to manufacture or advertise child pornography.

STATUTORY AUTHORITY

8. In my capacity as an investigator of criminal violations relating to child exploitation and child pornography, I have become familiar with the following federal statutes:

a. Child Exploitation Enterprise, 18 U.S.C. § 2252A(g), which makes it a crime to engage in a child exploitation enterprise, defined as including when a

person violates chapter 110 (except for sections 2257 and 2257A) as a part of a series of felony violations constituting three or more separate incidents and involving more than one victim, and commits those offenses in concert with three or more other persons.

b. Advertisement of Child Pornography, 18 U.S.C. § 2251(d), which makes it unlawful to knowingly make, print, or publish, or cause to be made, printed, or published, any notice or advertisement seeking or offering to receive, exchange, buy, produce, display, distribute, or reproduce, any visual depiction, if the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct, and such notice or advertisement is transported using any means or facility of interstate of foreign commerce or in or affecting interstate or foreign commerce by any means including by computer.

c. Transportation of Child Pornography, 18 U.S.C. § 2252A(a)(1), which makes it unlawful for someone to knowingly mail, or transport or ship using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer, any child pornography.

d. Receipt and Distribution of Child Pornography, 18 U.S.C. § 2252A(a)(2)(A), which makes it unlawful for someone to knowingly receive or distribute any child pornography that has been mailed, or using any means or facility of interstate or foreign commerce shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

e. Possession of Child Pornography, 18 U.S.C. § 2252A(a)(5)(B), which makes it unlawful for someone to knowingly possesses, or knowingly accesses with intent to view, any book, magazine, periodical, film, videotape, computer disk, or any other material that contains an image of child pornography that has been mailed, or shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any

means, including by computer, or that was produced using materials that have been mailed, or shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

f. Pursuant to 18 U.S.C. § 2256(8), Child Pornography is defined as "any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where - (A) the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct; . . . . or (C) such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct."

g. Pursuant to 18 U.S.C. § 2256(1), the term "minor," is defined as "any person under the age of eighteen years."

DEFINITIONS

9. The following definitions apply to this Affidavit:

a. "Child erotica," as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not, in and of themselves, obscene or that do not necessarily depict minors in sexually explicit poses or positions.

b. "Child pornography," as used herein, includes the definitions in 18 U.S.C. §§ 2256(8) and 2256(9) (any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct). See 18 U.S.C. §§ 2252 and 2256(2).

c. "Visual depictions" include undeveloped film and videotape, data stored on computer disk or by electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in permanent format. See 18 U.S.C. § 2256(5).

d. "Sexually explicit conduct" means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, anal genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any persons. See 18 U.S.C. § 2256(2).

e. "Computer," as used herein, is defined pursuant to 18 U.S.C. § 1030(e)(1), as "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device."

f. "Computer hardware," as used herein, consists of all equipment which can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

g. "Computer software," as used herein, is digital information which can be interpreted by a computer and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic, or other

digital form. It commonly includes programs to run operating systems, applications, and utilities.

h. The terms "records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (DVDs), personal digital assistants (PDAs), multimedia cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

i. "Computer passwords and data security devices," as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha numeric characters) usually operates a sort of digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Digitally coded data security software may include programming code that creates "test" keys or "hot" keys, which perform certain pre set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby trap" protected data to make it inaccessible or unusable, as well as reverse the progress to restore it.

j. "Internet Protocol address" or "IP address" refers to a unique number used by a computer to access the Internet. IP addresses can be dynamic, meaning that the Internet Service Provider (ISP) assigns a unique and different

number to a computer every time it accesses the Internet. IP addresses might also be static, if an ISP assigns a user's computer a particular IP address which is used each time the computer accesses the Internet.

k. "Bulletin Board" means an Internet-based website that is either secured (accessible with a password) or unsecured, and provides members with the ability to view postings by other members and make postings themselves. Postings can contain text messages, still images, video images, or web addresses that direct other members to specific content the poster wishes. Bulletin boards are also referred to as "internet forums" or "message boards." A "post" or "posting" is a single message posted by a user. Users of a bulletin board may post messages in reply to a post. A message "thread," often labeled a "topic," refers to a linked series of posts and reply messages. Message threads or topics often contain a title, which is generally selected by the user who posted the first message of the thread. Bulletin boards often also provide the ability for members to communicate on a one-to-one basis through "private messages." Private messages are similar to e-mail messages that are sent between two members of a bulletin board. They are accessible only by the user who sent/received such a message, or by the Website Administrator.

BACKGROUND OF "WEBSITE X"

10. The United States government, including the United States Department of Homeland Security, Homeland Security Investigations (HSI), is investigating violations concerning child exploitation. The investigation concerns possible violations by known and unknown individuals of, inter alia, 18 U.S.C. §§ 2251(d), 2251(e), and 2252A, as described above.

11. HSI agents opened an investigation in an attempt to infiltrate high level child pornography rings/websites and target the administrators of said websites. At

the present time, this investigation involves multiple individuals, believed to be residing across the United States and abroad, who were users of an Internet-based bulletin board that operated on an anonymous online network. That website, hereinafter referred to as "Website X," operated from approximately July 2015 until approximately November 2016.[1] HSI has been investigating the users of Website X, and more specifically the known and unknown individuals who own and administrate this website. These individuals worked together to maintain Website X, fund the hosting of Website X, and knowingly advertise the sexual exploitation of children.

THE NETWORK

12. Your affiant is personally aware that "Website X" operated on a particular network ("the Network") available to Internet users. The Network is designed to facilitate anonymous communication over the Internet. To access the Network, a user installs computer software that is publicly available, either by downloading software to the user's existing web browser, downloading free software available from the Network's administrators, or downloading a publicly-available third-party application. The Network's software protects users' privacy online by bouncing their communications around a distributed network of relay computers run by volunteers all around the world, thereby masking the user's actual IP address, which could otherwise be used to identify a user. Because of the way the Network routes communication

[1] The actual names of the websites described herein are known to law enforcement. Investigation into the users of the sites remains ongoing and disclosure of the names of the sites would potentially alert users to the fact that law enforcement action is being taken against the sites, potentially provoking users to notify other users of law enforcement action, flee, or destroy evidence.

through other computers, traditional IP identification techniques are generally not viable in identifying computers operating on the Network.

13. Websites that are accessible only to users operating within the Network can be set up within the Network. "Website X" was one such website. These websites operate the same as regular public websites with one critical exception—the IP address for the web server is hidden and instead is replaced with a Network-based web address. To access "Website X," a user had to either know the exact web address or discover its exact web address, for example, from other users or from servers on the Network that maintain indexes of known websites. Moreover, because neither a user nor law enforcement can identify the actual IP address of the web server, it is not possible to determine through public lookups where the computer that hosts the website is located. Accordingly, it is not possible to obtain data detailing the activities of the users from the website server through public lookups.

14. I have reviewed postings that were accessible to members of Website X captured by other HSI agents in an undercover capacity, using accounts registered by law enforcement agents and accounts obtained via consent of investigation subjects, and I have spoken with agents who have viewed and captured the postings. Website X was dedicated to the advertisement, distribution, and receipt of child pornography. As of November 2016, Website X had over 27,000 registered users some of whom actively posted new child exploitation content and who engaged in online discussions involving the sexual exploitation of minors. Website X had various sections containing forums and sub forums in which members posted messages and images for other members to

view. For example, there were sections labeled "Girls" and "Boys" and within each of these sections were several forums, including: "Pre-teen Hardcore," "Pre-teen Softcore/Non-nude," "Model/Producer section," "Babies and toddlers" and "Requests." Typical posts contained text, preview images of child pornography or erotica available for download, links to external file sharing websites from which the advertised images or videos could have been downloaded, and any required passwords.

15. Members and the administrators routinely identified themselves by aliases or screen names on Website X and other forums or internet-based platforms on which these individuals communicate. This allows other individuals to gain familiarity and build relationships with each other while maintaining anonymity so as to avoid detection by law enforcement.

16. To become a Member of Website X, an administrator or moderator of the board had to approve a user, by reviewing their "application post." A user was only approved to be a Member after they applied for full membership by creating a post containing child pornography. This posting was typically referred to as the application post. If the posting did not clearly depict minors in sexually explicit images and videos, or other posting rules were not followed, a user was not approved for membership in the Website X.

17. Website X also had a "VIP" section, which was accessible only to users who uploaded new or originally produced images or videos of child pornography. A website administrator reviewed and approved the uploaded material and determined

whether to approve the applicant for membership in the VIP section. When a member posted images or videos of child pornography, Website X required the member to post the material by way of an off-site file hosting website (i.e., another website, separate from Website X, where users can upload password-protected files for others to download). The member was required to post a "preview" image or screen shot of the child pornography and a functioning hyperlink to the file on Website X. The sexually explicit material must have been password-protected, and the member must have provided the password in his posting so that other members could access the child pornography from the file hosts sites.

USER "PANTYLVR's" ACTIVITY ON WEBSITE X

18. According to a review of postings on Website X documented by HSI agents who reviewed those postings while accessing Website X in an undercover capacity, on November 26, 2015, the user "Pantylvr" posted a message in the "New Joiner," "Successful Applications" section entitled "Bedtime sleeper 6yo." The posting included a preview image depicting a prepubescent female child sleeping with her shirt pulled up to expose her breast and her hand on her genital area, which is covered by underpants. The posting included a link to a .rar file[2] containing 41 images located on an external file hosting website. Pantylvr stated below this image preview, "Yes, the panties come off! Cumshot on chest included. Its [sic] still one of my favorite sets." "Pantylvr" also stated, "Please enjoy and hope its [sic] good enough for approval."

[2] A .rar file is a file saved in a type of proprietary archive file format that supports data compression, error recovery and file spanning.

Later that day, a moderator of the forum approved "Pantylvr's" application post stating, "Hi Pantylvr! Welcome to [Website X]. Your application meets our requirements. You are now activated and free to browse our forum."

19. On November 27, 2015, "Pantylvr" posted a message on Website X entitled "Hello" and stated, "thanks to admin for approving my membership so fast. this looks like a great place. hope i [sic] can contribute some things. thanks for everyones [sic] contributions."

20. On November 30, 2015, "Pantylvr" posted two photo arrays[3] of preview images with links to the full videos on an external file hosting website in the "Girls", "Pre-teen Hardcore", "Videos" section of Website X. The posting is entitled "Pink Sleepy Vids (2)" and "Pantylvr" stated "This is my first content post here other than my application post. Hope everyone enjoys. Im [sic] also looking for more of this girl...i [sic] know there is more out there." The first set of images depicts a sleeping minor female and an adult male appearing to masturbate and ejaculate on her face. The second set of images depicts a prepubescent female with her underpants removed, exposing her genitals as the focal point of the image and an adult male appears to masturbate and ejaculate on her bare chest area.

21. On November 30, 2015, "Pantylvr" posted a question in the "Requests" section of the "Girls" forum entitled, "(update)who are they? Please help." Within that message,"Pantylvr" posted five pictures depicting a prepubescent minor female

[3] A "photo array" or "storyboard" is a series of still images from a video file that show different parts of the video and is intended to give the viewer an idea of the video's content.

sleeping. In two of the photos, the minor's underpants are removed to expose her genitals. In the other photos, her underpants are partially removed. "Pantylvr" stated, "I have no idea who they are but there has to be a set out there. I saw several NN[4] panty pics on imgsrc[5] a few months back but never saved them like a dumbass. Looks like two girls in the same bed with pics taken on multiple nights. Any help is greatly appreciated. I know im[sic] new here and just made my first content post a few minutes ago and will post when I can. This is a great place."

22. On December 3, 2015, "Pantylvr" made a post in the "Videos" section of the "Pre-teen Hardcore," "Girls" forum entitled, "Hayley Vids (3)." "Pantylvr" stated "There are 3 vids in this rar but could not get vid cap maker to work on the one file. Hay vids 1, 2, and 4. Would love to see more of her vids... i[sic] know they exist. Used to have more but had crash. Also looking for pictures from this producer...used to have them too. Any addition to this thread would be appreciated." The two photo arrays that "Pantylvr" posted with this message depict a prepubescent female minor sleeping, with no underpants and her genitals exposed to the camera. In the second array, an adult male's hand digitally penetrates the minor's genitals.

---

[4] I know based on my training and experience that "NN" means non-nudes, in this context.

[5] IMGSRC is an image hosting website that allows users to register with a user name and email address. Individuals with an account can post images on the site that can be viewed publically or can post images or folders of images that require a password to view. Individuals with an account can also post comments about images posted by other users. IMGSRC has historically been used by individual posting or seeking to post and view images of child pornography. The administrators of the IMGSRC website actively ban users for posting child pornography.

23. On January 23, 2016, "Pantylvr" made a post in the "Cam" section of the "Girls" forum entitled, "HOT strip 10-11yr." In this post, "Pantylvr" stated, "This was new to me so maybe its[sic] new for a few others here. Found this all the way down in the reviewed applications section and figured its worth posting here the proper way. Maybe this girls put on more shows too. Shes[sic] hot." The photo array depicts a prepubecent female minor in increasing stages of undress until she is fully nude.

24. As of November 8, 2016, "Pantylvr" was ranked as a VIP user of Website X. He made several more posts and comments to the website between November 2015 and June 2016.

25. HSI agents have also accessed in an undercover capacity another website on the Network, hereinafter referred to as Website Y. Website Y is dedicated to the advertisement, distribution, and receipt of child pornography and is still operating on the Network. Like Website X, Website Y is a membership-based online forum where users actively post new child exploitation content and engage in online discussions involving the sexual exploitation of minors. Typical posts include preview images and links to child pornography that can be downloaded from a third-party file-sharing website. Website Y has various sections containing forums and sub-forums, including sections labeled "Girls," "Boys," "Pre-teen," "Fetish," "Webcams," and "Baby and toddler." User "LovePanties" is a moderator and frequent contributor to Website Y and has posted to Website Y as recently as December 2016. As noted above, based upon my training and experience and consultation with experienced investigators of online child pornography groups, it is common for child pornography offenders who participate in

organized child pornography groups to maintain similar screen name across websites, in order to build and maintain credibility within online child exploitation communities such as Website X. Based on my training and experience and the following information, I believe user "Pantylvr" and user "LovePanties" to be the same individual:[6]

a. On August 20, 2016, user "LovePanties" sent a private message to another user on Website Y. In that message, "LovePanties" said:

> . . . Ive [sic] sent you a private message before.... probably on [Website X] under pantylvr.
> Anyways, I was just sending you a pm to see if you wanted to chat sometime or even exchange rare material.... i believe I have a fairly decent collection. Unreleased Sarah/steph, RF, SweatPea, Jada, Luna, to name a few. . . I have a huge little girl panty fetish and your avatar really gets me going ;)

b. On August 28, 2016, user "Pantylvr" sent a private message to another user on Website X. In that message, "Pantylvr" said:

> "Thanks for your awsome [sic] cam thread. Please keep up the great posts.My new fav cam girl is from esp455.mp4 which you posted, and anon007 also posted 3 additional clips of her on [Website Y] . . . I have been really starting to love these cam vids more than the hardcore material as of late... especially with the awsome [sic] quality and English speaking hot preteens putting on the shows. Would love to chat sometime or even share. Hope to hear from you soon. take care ps.... this is lovepanties from [Website Y] ;)"

IDENTIFICATION OF "PANTYLVR"

26. In October, 2016, special agents with HSI Boston were involved in the investigation and arrests of two high ranking members of Website X. These two people

[6] The user named Website X and Website Y in the bracketed portions of the below posts.

are identified in this search warrant affidavit as "TARGET A" and "TARGET B." These individuals were arrested and computer forensic examinations of their computer media were conducted, which led to the discovery of numerous conversations from an online messaging service. This online messaging service is encrypted, and users are identified by an ID, which consists of a long series of letters and numbers. Users can assign an alias to this ID so they can easily identify other users they communicate with. On TARGET A's media devices, a particular ID in his friend's list was given the alias "pantylvr." On TARGET B's devices, the same ID in his friend's list was also given the alias "pantylvr." The messaging service also allows a user to include a tagline, referred to as a "public information status," which other users can see. The tagline associated with "pantylvr" on both TARGET A's and TARGET B's devices was "Stealing Panties."

27. Review of that information, including numerous private chats between "TARGET A" and "Pantylvr" and "TARGET B" and "Pantylvr," revealed that "Pantylvr" provided numerous clues about his identity. For example, in a September 3, 2016 chat found on "TARGET A's" computer, "Pantylvr" and TARGET A discussed a known child pornography series referred to as "Ms. Alli:"

TIME UTC	USERNAME	MESSAGE
9/3/16 3:59:21	[TARGET A]	Ohh, Ms Allie
9/3/16 3:59:22	[TARGET A]	I do, heh
9/3/16 3:59:35	[TARGET A]	So sex, lord
9/3/16 3:59:38	[TARGET A]	sexy*
9/3/16 4:00:02	**"Pantylvr"**	**i have a special connection to that set**
9/3/16 4:00:07	**"Pantylvr"**	**set 45**
9/3/16 4:01:20	[TARGET A]	ohh, yeah?
9/3/16 4:01:24	[TARGET A]	How is that?)

9/3/16 4:01:26	[TARGET A]	:)
9/3/16 4:01:47	**"Pantylvr"**	**that was my custom set that i requested**
9/3/16 4:01:48	[TARGET A]	besides the great panty shots :P
9/3/16 4:01:54	[TARGET A]	Ohh yeah? I love!
9/3/16 4:01:55	[TARGET A]	heh
9/3/16 4:01:59	**"Pantylvr"**	**i paid 300 cash for him to shoot that**
9/3/16 4:02:28	**"Pantylvr"**	**i ordered the clothes, sent them to him, requested poses, setting, ect**
9/3/16 4:02:45	[TARGET A]	wow, lol, that's awesome
9/3/16 4:02:55	[TARGET A]	love the cloths and shot
9/3/16 4:03:04	[TARGET A]	it really is perfect
9/3/16 4:03:05	[TARGET A]	lol
9/3/16 4:03:14	[TARGET A]	butt + awesome panties and bra
9/3/16 4:03:31	**"Pantylvr"**	**then i had alli wear the panties for a day then the producer sent the socks, bra and panties back to me**
9/3/16 4:03:46	**"Pantylvr"**	**it was great**

28. On or about August 4, 2016, HSI was notified that a foreign law enforcement agency had identified the location of the computer server on which Website X was hosted and the private hosting company that owns that server. The foreign law enforcement agency reported to HSI that they had reviewed data provided by the owner of the server and confirmed that Website X is located on that server. The private hosting company voluntarily provided copies of Website X data to foreign law enforcement, who shared that data with HSI. In October and November 2016, foreign law enforcement seized Website X and Website Y. HSI has received and reviewed data from the seizures of these websites by foreign law enforcement.

29. The data seized by foreign law enforcement and shared with HSI, contains a private message from user "LovePanties" to another user on Website Y sent at 11:01 PM CDT on September 14, 2016, in which user "LovePanties" states:

> "thanks for sharing the Miss Alli custom set. I wish there were more original/full sets like that out there of her. When her site was open I was responsible for set 45.... I ordered it as a custom. I mailed Rebel Shooter the outfit and described exactly what I wanted as the scene. I requested it to be shot in Alli's bedroom. Her real name is [redacted] by the way.... look in set 45 at her backpack.... its faint but you can read it. My set was over 100 pictures as well but only a portion were released on her site for public purchase. Pictures were over 1mb each. Several years back I had a crash and lost all my stuff, including my custom set..... never was able to get it back either :(I emailed Rebel about it but he claimed there was no way for me to prove my identity with him since he did not keep records of transactions once they were completed. He wouldnt [sic] resend me the originals. What Rebel Shooter did was embed your personal information into the pictures data so he was able to tell if you were around sharing your custom set originals. If you opened an original picture from any site purchase in notepad, you would be able to see the buyer's information. Anyways, just thought i [sic] would thank you for sharing the larger set of Alli."

30. The individual responsible for creating the "Miss Alli" series, who went by the user name "Rebel Shooter," was arrested by the United States Postal Inspection Service (USPIS) in 2012. HSI obtained from USPIS Detroit one of the images from the evidence in that case with the file name "Alli Site Set 45 (27).JPG." The image depicts a girl who appears to be about 7 to 9 years old, fully clothed and posed in a sitting position with her hand under her chin. As noted in the above posting by "LovePanties," "Rebel Shooter" embedded personal information of the purchaser of the

child pornography images in the image itself. Examination of the image "Alli Site Set 45 (27).JPG " revealed the following metadata[7] associated with that image:

> Alli Site Set 53 .CIC P:Rebel_Shooter..Allen Anderson.BB.Shipping Address.PO Box 100741.Cudahy, WI 53110.Hunt 5421.
>
> DateTimeOriginal: 2008:04:18 22:34:30
>
> CreateDate: 2008:04:18 22:34:30

31. HSI obtained, via USPIS, records from the Cudahy, Wisconsin post office which show that on April 2, 2008—the same month the Ms. Alli Set 45 was created based on the metadata above—Brett BEDUSEK applied for P.O. Box 100741, Cudahy, WI 53110. On the application for this post office box, the registrant information included his residence, which is the SUBJECT PREMISES, as well as the following additional information:

> Brett Bedusek 5412 S. Hately Ave. Cudahy WI, 53110
> Telephone 414-467-1250 Driver's License B3220618406505.

32. In chats with "TARGET B" found on TARGET B's computer, "Pantylvr" revealed the following information about himself:

a. On May 18, 2016, "Pantylvr" said he weighed approximately 200 lbs. According to BEDUSEK's information from the Wisconsin sex offender registry, he weighs approximately 235 lbs.

b. On June 18, 2016, "Pantylvr" said he lived in the Midwest.

c. On March 3, 2016, "Pantylvr" said that he was 8 hours away from Kansas. Cudahy, Wisconsin is 8 hours and 18 minutes from Kansas City, Kansas,

[7] Metadata is additional information that is stored within a graphic image, including information such as make and model of the camera and date and time picture was taken. Metadata is customizable.

according to the online utility Google maps, which based upon my training and experience is a widely-used and accurate source of location information.

d. On April 22, 2016; May 8, 2016; May22, 2016; and June 6, 2016, "Pantylvr" discussed driving his truck and going fishing. According to Wisconsin department of motor vehicle records, BEDUSEK had a Dodge Ram truck last registered in his name in 2012 bearing license plate number "BBFISHIN." In addition, an open-source Internet search for individuals believed to be relatives of BEDUSEK based on public records led to a Facebook profile in the name of Brett Bedosik. The profile picture on that Facebook profile shows an adult male individual holding a large fish. Further open-source Internet searches revealed that an email address of bbfishin@wi.rr.com is associated with "BRETT BEDUSEK" on an online fishing forum.

e. On May 5, 2016, "Pantylvr" stated that he has a state felony conviction, but claimed that it was not "pedo related." According to publicly available court records, on July 13, 2009, BEDUSEK was arrested in the Eastern District of Wisconsin for charges related to the receipt and possession of child pornography in case number, 09-cr-00181. A search warrant was executed at the SUBJECT PREMISES at that time. On June 6, 2011, BEDUSEK was sentenced to 56 months of incarceration, followed by 10 years of supervised release.

f. Publicly available Bureau of Prisons records show BEDUSEK was released on June 12, 2015. "Pantylvr" first posted on Website X on November 26, 2015. Analysis of Website X data determined that "Pantylvr's" password on Website X is "imback."

g. On March 18, 2016, "Pantylvr" stated that he "might have a business degree." During the July 2009 search that led to BEDUSEK's arrest, HSI agents observed a University of Wisconsin diploma for a business degree at the SUBJECT PREMISES.

h. On April 17, 2016 11:23 p.m. CDT, "Pantylvr" discussed with TARGET B on the encrypted messaging services that he had purchased a new

"Digiland Tablet" and that he was not supposed to be using an unmonitored digital device.

- The chat contents include:

> Pantylvr: so.... i [sic] went out and bought a new tablet.... same kind and all[8]
> Pantylvr: tonight when i [sic] was using it, i [sic] just switched out the old one with the new one
> Pantylvr: now she holds the new one, while i [sic] got mine toy back
> . . .
> Pantylvr: im [sic] not supposed to be on internet since they know i [sic] have an issue with being a pedo
>
> TARGET B: who is "she"?
> . . .
> Pantylvr: mom
> . . .
> Pantylvr: its [sic] not about pretending im [sic] doing something on a computer...im [sic] not supposed to be using one unmonitored at all
> Pantylvr: ;) hence the hidden tablet

- Records provided by Best Buy in response to legal process show that a DL808W 8 INCH WINDOWS TABLET WITH 32G, a DigiLand tablet, was purchased with cash on April 17, 2016, at the Best Buy store #25 in Greenfield, Wisconsin. According to Google Maps, that particular Best Buy store is a 16 to 17 minute drive from Cudahy, Wisconsin. A representative of Best Buy also informed an HSI Boston special agent that, according to records associated with a Best Buy rewards program, Brett BEDUSEK made six purchases at Best Buy Store #25 in Greenfield, Wisconsin, between January 31, 2016, and January 30, 2017.

[8] On March 26, 2016 3:56 p.m. CDT, "Pantylvr" had told TARGET B that he was using a "digiland tablet."

- According to publicly available court records, a condition of BEDUSEK's supervised release in case number 09-cr-00181 includes that he comply with the United States Probation Office's Computer Monitoring Program and install filtering software on any device he possesses or uses. He is also required to allow the probation office periodic unannounced examinations of his computer equipment to conduct a more thorough inspection.

j. According to data received from foreign law enforcement and shared with HSI, on May 14, 2016 at 4:30 a.m. CDT "LovePanties" on Website Y, sent TARGET B a private message following up on a May 11, 2016, encrypted chat message (as "Pantylvr") in which they discussed TARGET B's access to a minor, his upcoming travel to see the minor and "panties" TARGET B could pose the minor in for the purpose of producing images of the minor and sharing with "Pantylvr." In this private message, "LovePanties" sent TARGET B a message containing two hyperlinks to specific panties available for online purchase via the website Walmart.com that TARGET B could purchase and dress the minor in. One of those hyperlinks was to the following URL: "*http://www.walmart.com/ip/Fruit-of-the-Loom-Girls-Cotton-Bikini-Panty-12-Pack/46349221*".

- On February 10, 2017, a Grand Jury subpoena from the Middle District of Tennessee was issued to Walmart Corporate Headquarters in Bentonville, Arkansas, requesting information about IP addresses of computers that accessed the URLs that "LovePanties" included in his private message to TARGET B. On February 24, 2017, Walmart provided information relating to the IP addresses that accessed the URL "*http://www.walmart.com/ip/Fruit-of-the-Loom-Girls-Cotton-Bikini-Panty-12-Pack/46349221*" between May 13, 2016 and May 15, 2016.

- Pursuant to Walmart's records, the user of a computer with IP address 65.31.180.1 searched for the words "Girls Panties" and accessed this link on May 13, 2017 at 9:10 p.m. CDT from a device using a Windows 8.1 operating system. That is the same operating system as the model of Digiland tablet that "Pantylvr" has stated he uses.
- Using Maxmind, a publically available geo-location tool for IP addresses, IP address 65.31.180.1 is registered to Time Warner and the subscriber is physically located near South Milwaukee, Wisconsin. Based on open-source Internet searches, an email address associated with BEDUSEK is bbfishin@wi.rr.com.[9]
- In response to legal process, Time Warner provided the following subscriber information for email address bbfishin@wi.rr.com:

Subscriber Name: Evette Bedusek

Subscriber Address: 5412 S. Hately Ave, Cudahy, WI 53110-2020

Service Type - RR HSD Activate Date: 5/11/2009
Deactivate Date: Still Active

User Name or Features: bbfishin@wi.rr.com, ebfishin@wi.rr.com,
BedusekInsurance@wi.rr.com,
BBEDUSEK@wi.rr.com

Phone number: (414)481-5702, (414)531-0869

Other Information: Current IP: 65.31.180.1
held since 07/31/15 14:51:14

[9] In this context, "rr" stands for roadrunner, a brand name used by Time Warner for its Internet service.

PRIOR INVESTIGATIONS INVOLVING BEDUSEK

33. The metadata from the Miss Alli series set 45, described above, includes other identifiers that are associated with BEDUSEK from a prior investigation: the name "Hunt5421" and the name "Allen Anderson."

34. In a 2008 investigation, HSI, then called Immigration and Customs Enforcement (ICE), identified the user of email account hunt5421@yahoo.com was connected to a profile on the website "iMGSRC.ru" with the user name "Hunt5421." In June 2009, the profile displayed the following:

> Real name: Hunt
> Email: hunt5421@yahoo.com
> Registered on:2006-12-19
> User info: Love them panties] NO FREE PASSES]]]] DON'T EVEN ASK] My passes
> have changed 1/22/09
> Albums of hunt5421 (19)
> Tagged under: bikini, bra, candid, daughter, family, girl, girls, little, panties, pool, preteen, swim, swimsuit, training bra, underwear, up skirt, young.

35. Based on a review conducted by prior HSI agents on that case, the majority of the images in each of the albums associated with the imgsrc user Hunt5421 would be considered child erotica, except for the images located in the album named, "Upskirt Cutie 6yo." This album had a total of twelve images of a female between the ages of 5 to 7 years of age. Eight images (IMG_0110.jpg, IMG_0106.jpg, IMG_0110.jpg, IMG_0106.jpg, IMG_0110.jpg, IMG_0106.jpg, IMG_0110.jpg, and IMG_0106.jpg) are explicit images of a preteen female's genital area.

36. On February 2, 2009, Yahoo responding to a Customs Summons provided this information from the Hunt5421@yahoo.com account:

Login Name: hunt5421
GUID: 7W2HGDZLKKRXOF6V6QG4WJMAME
Properties Used: Flickr / Mail / Web Messenger
Yahoo Mail Name: Hunt5421@yahoo.com
Registration IP Address: 64.179.61.99
Account created: Tue Dec 05 17:53:04 2006 GMT
Other Identities: hunt5421 (Yahoo] Mail)
Full Name: Mr Allan Anderson
Address: (BLANK)
City: Beverly Hills
State: CA
Country: United States
Zip/Postal Code: 90210
Time zone: pt
Birthday: March 25, 1984
Gender: Male
Account Status: Active

37. Based on my training and experience, information provided by a Yahoo user pertaining to the fields of name, address, city, state, country, postal code, birthday and gender are provided by the user and not verified by Yahoo. On April 14, 2009, Yahoo Inc., in response to a search warrant, produced subscriber records pertaining to hunt5421@yahoo.com which showed that the IP address 216.47.252.11 was used four hundred and six times in one year to access the hunt5421@yahoo.com account. On June 4, 2009, One Communications, in response to a customs summons, detailed that the IP address: 216.47.252.11 was subscribed to by Bedusek Agency, Inc. at 5656 Packard Avenue, Cudahy, Wisconsin 53110. According to open internet searches, The Bedusek Agency, Inc was an insurance agency in Milwaukee County which was owned and

operated by Jay Bedusek. According to public records, Jay Bedusek also owns the SUBJECT PREMISES.

38. According to publically available court records, on September 17, 2010, Brett BEDUSEK pled guilty to receipt of child pornography. As part of his plea agreement in that case, he admitted to receiving an image of a young female, approximately 6-8 years old, laying nude on a red blanket wearing pink underwear with white dots, the hand of a white male exposing the minor female's vagina, in case number 09-cr-00181 (EDWI). HSI agents executed a search warrant at BEDUSEK's residence, the SUBJECT PREMISES, in July 2009. BEDUSEK admitted as part of his plea agreement that during the search warrant, inside the doorway at the SUBJECT PREMISES, agents located small girls' underpants and socks in a locked red metal toolbox, along with non-pornographic pictures and videos of young girls. BEDUSEK admitted that some of the underpants were in an envelope that had been mailed to him at a Cudahy post office box. BEDUSEK further admitted that on BEDUSEK's computer, agents observed an image of young girl approximately 10 years old, exposing her genital area and breasts saved as the wallpaper of his computer. A computer forensic examiner located numerous deleted pornographic images depicting minors engaged in sexually explicit conduct on his computer and a thumb drive located in his bedroom. BEDUSEK agreed to be interviewed and confessed to receiving and possessing over 600 images of child pornography.

PROBABLE CAUSE THAT "PANTYLVR" USES HIS TABLET AT THE "SUBJECT PREMISES"

39. In chats with "pantylvr" found on TARGET B's computer "pantylvr" explained that he uses his tablet at home but has to use it at night or when his mother is not home:

pantylvr:	anyways, i [sic] just wont be online anymore unless she isn't [sic] home, or im[sic] in bed for the night
	. . .
pantylvr:	the only diff u will see is that ill [sic] be online about two hrs later than normal.... thats [sic] it
pantylvr:	ill [sic] still be on at night just like now
pantylvr:	im [sic] just not going to use it during daylight hrs
	. . .
pantyvlr:	i [sic] was in my room and she snuck up on me as she walked by and the screen was in view at the right angle
pantylvr:	yes, i [sic] will hide the tablet better now too

40. HSI Agents performed an analysis of posts on Website Y by the individual using the screen name "LovePanties", this analysis included converting all the post times to CST. Based on the analysis of 197 posts by the individual using the screen name "LovePanties" the Agents learned that this individual made **from April to December 2016, 25 posts between 8:00 a.m.-7:00 p.m., 73 posts between 8:00 p.m.-2:00 a.m. and 99 posts between 3:00 a.m.-7:00 a.m.** Therefore the this individual is more than likely using device the SUBJECT PREMISES in the late evening to early morning hours.

COMPUTERS AND CHILD PORNOGRAPHY

41. Based upon my training and experience, I know that computers and computer technology have revolutionized the way in which individuals interested in

child pornography interact with each other. In the past, child pornography was produced using cameras and film (either still photography or movies). The photographs required darkroom facilities and a significant amount of skill in order to develop and reproduce the images. There were definable costs involved with the production of pornographic images, and to distribute these images on any scale required significant resources and significant risks. The photographs themselves were somewhat bulky and required secure storage to prevent their exposure to the public and/or law enforcement. The distribution of these wares was accomplished through a combination of personal contacts, mailings and telephone calls.

42. The development of computers has radically changed the way that child pornographers obtain, distribute and store their contraband images and videos. Computers basically serve five functions in connection with child pornography: access, production, communication, distribution, and storage.

43. Child pornographers can now convert paper photographs taken with a traditional camera (using ordinary film) into a computer readable format with a device known as a scanner. Moreover, with the advent, proliferation and widespread use of digital cameras, the images can now be transferred directly from a digital camera onto a computer using a connection known as a USB cable or other device. Digital cameras have the capacity to store images and videos indefinitely, and memory storage cards used in these cameras are capable of holding hundreds of images and videos. A device known as a modem allows any computer to connect to another computer through the

use of telephone, cable, or wireless connection. Electronic contact can be made to literally millions of computers around the world.

44. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. The size of the electronic storage media, that is, the hard disk drive used in home computers has grown tremendously within the last several years. These hard disk drives can store hundreds of thousands of images at very high resolution.

45. The World Wide Web of the Internet affords collectors of child pornography several different venues for obtaining, viewing and trading child pornography in a relatively secure and anonymous fashion.

46. Collectors and distributors of child pornography frequently use online resources to retrieve and store child pornography, including services offered by Internet Portals such as Yahoo!, Hotmail, and Google, among others. The online services allow a user to set up an account with a remote computing service that provides email services as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet. Evidence of such online storage of child pornography is often found on the user's computer. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer in most cases.

47. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional, i.e., by saving an email as a file on the computer or

saving particular website locations in, for example, "bookmarked" files. Digital information, images and videos can also be retained unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places (e.g., temporary files or ISP client software, among others). Often, a computer will automatically save transcripts or logs of electronic communications between its user and other users which have occurred over the Internet. These logs are commonly referred to as "chat logs." Some programs allows computer users to trade images while simultaneously engaging in electronic communications with each other. This is often referred to as "chatting," or "instant messaging." Based on my training and experience, I know that these electronic "chat logs" often have great evidentiary value in child pornography investigations, as they record communications in transcript form, show the date and time of such communications, and also may show the dates and times when images of child pornography were traded over the Internet. In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. A forensic examiner often can recover evidence suggesting whether a computer contains peer to peer software, when the computer was sharing files, and some of the files which were uploaded or downloaded. Such information is often maintained on a computer for long periods of time until overwritten by other data.

SEARCH AND SEIZURE OF COMPUTER SYSTEMS

48. Based on my training and experience, I know that searches and seizures of evidence from computers commonly require law enforcement agents to download or

copy information from the computers and their components, or seize most or all computer items (computer hardware, computer software, and computer related documentation) to be processed later by a qualified computer expert in a laboratory or other controlled environment. This is almost always true because of the following:

a. Computer storage devices (like hard drives, compact discs [CD], diskettes, tapes, and others) can store the equivalent of thousands of pages of information. Especially when the user wants to conceal criminal evidence, he or she often stores it in random order with deceptive file names. This requires searching authorities to examine all the stored data to determine whether it is included in the warrant. This sorting process can take days or weeks, depending on the volume of data stored, and it would be generally impossible to accomplish this kind of data search on site; and

b. Searching computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert should analyze the system and its data. The search of a computer system is an exacting scientific procedure which is designed to protect the integrity of the evidence and to recover hidden, erased, compressed, password protected, or encrypted files. Since computer evidence is extremely vulnerable to tampering or destruction (which may be caused by malicious code or normal activities of an operating system), the controlled environment of a laboratory is essential to its complete and accurate analysis.

CHARACTERISTICS COMMON TO INDIVIDUALS WHO ACCESS WITH INTENT TO VIEW AND TRADE CHILD PORNOGRAPHY

47. Based on my experience, training, and conversations with other experienced agents who investigate cases involving the sexual exploitation of children, I know that certain common characteristics are often present in individuals who access with intent to view, receive, and distribute child pornography. I have observed and/or learned about the reliability of these commonalities and conclusions involving individuals who collect, produce and trade images of child pornography. Based upon my training and experience, and conversations with other experienced agents in the area of investigating cases involving sexual exploitation of children, I know that the following traits and characteristics are often present in individuals who trade and collect child pornography:

a. Many individuals who traffic in and trade images of child pornography also collect child pornography. Many individuals who collect child pornography have a sexual attraction to children. They receive sexual gratification and satisfaction from sexual fantasies fueled by sexually explicit depictions of children.

b. Many individuals who collect child pornography collect sexually explicit materials, which may consist of photographs, magazines, motion pictures, video tapes, books, slides, computer graphics or digital or other images for their own sexual gratification. Most of these individuals also collect child erotica, which may consist of images or text that do not rise to the level of child

pornography but which nonetheless fuel their deviant sexual fantasies involving children.

c. Many individuals who collect child pornography often seek out like minded individuals, either in person or on the Internet, to share information and trade depictions of child pornography and child erotica as a means of gaining status, trust, acceptance, and support. This contact also helps these individuals to rationalize and validate their deviant sexual interest and associated behavior. The different Internet based vehicles used by such individuals to communicate with each other include, but are not limited to, Peer to Peer (P2P), email, email groups, bulletin boards, Internet Relay Chat Rooms (IRC), newsgroups, instant messaging, and other similar vehicles.

d. Many individuals who collect child pornography maintain books, magazines, newspapers and other writings (which may be written by the collector), in hard copy or digital medium, on the subject of sexual activities with children as a way of understanding their own feelings toward children, justifying those feelings and finding comfort for their illicit behavior and desires. Such individuals often do not destroy these materials because of the psychological support that they provide.

e. Many individuals who collect child pornography often collect, read, copy or maintain names, addresses (including email addresses), phone numbers, or lists of persons who have advertised or otherwise made known in publications and on the Internet that they have similar sexual interests. These

contacts are maintained as a means of personal referral, exchange or commercial profit. These names may be maintained in the original medium from which they were derived, in telephone books or notebooks, on computer storage devices, or merely on scraps of paper.

f. Many individuals who collect child pornography rarely, if ever, dispose of their sexually explicit materials and may go to great lengths to conceal and protect them from discovery, theft, or damage. These individuals view their sexually explicit materials as prized and valuable materials, even as commodities to be traded with other like minded individuals over the Internet. As such, they tend to maintain or "hoard" their visual depictions of child pornography for long periods of time in the privacy and security of their homes or other secure locations. Based on my training and experience, as well as my conversations with other experienced law enforcement officers, I know that individuals who possess, receive, and/or distribute child pornography by computer using the Internet often maintain and/or possess the items listed in Attachment B.

48. There is probable cause to believe BEDUSEK is "pantylvr" based on the information outlined above. This individual meets the characteristics of a child pornography collector in the following ways:

a. According to publically available court records, during the search of the SUBJECT PREMISES in July 2009 for the investigation that led to Bedusek's conviction and incarceration for receipt of child pornography, in 09-cr-00181 (EDWI), agents located small girls' underpants and socks in a locked red

metal toolbox, along with non-pornographic pictures and videos of young girls. On Bedusek's computer, agents observed an image of young girl approximately 10 years old, exposing her genital area and breasts saved as the wallpaper of his computer. A computer forensic examiner located numerous deleted pornographic images depicting the minors engaged in sexually explicit conduct on his computer and a thumb drive located in his bedroom, as outlined in paragraph 38 above.

b. "Pantylvr" joined and participated in multiple child pornography websites.

c. "Pantylvr" solicited the customized production of child pornography images.

d. In a chat, "pantylvr" stated that when "caught" by his mother for looking at child pornography on his tablet, he purchased a new one and swapped it with the one his mother confiscated from him that contained his collection of child pornography so that he could continue his illegal activities, as referenced in paragraph 32(h) above.

CONCLUSION

49. Based on the foregoing, I have probable cause to believe that Brett BEDUSEK has used or is using one or more computers or electronic storage media located at 5412 S. Hately Ave, Cudahy, WI, more fully described in Attachment A to this affidavit, to among other things, distribute, receive and possess child pornography. Therefore, I have probable cause to believe that one or more individuals, using the

residence described above, has violated 18 U.S.C. §§ 2251, 2252 and 2252A. Additionally, I have probable cause to believe that fruits, evidence and instrumentalities of violations of 18 U.S.C. §§ 2251, 2252 and 2252A, including computers and other electronic storage external hard drive and media containing images or videos of child pornography, and the items more fully described in Attachment B to this affidavit (which is incorporated by reference herein), will be located in this residence or on his person.

50. Accordingly, I respectfully request a search warrant be issued by this Court authorizing the search of the residence described in Attachment A, the seizure of the items listed in Attachment B.

REQUEST FOR AUTHORITY FOR NO-KNOCK WARRANT

51. While reviewing the forums available to members on Website X, HSI undercover agents have observed extensive discussion threads on the website where encryption and avoidance of law enforcement detection are discussed.

52. For example, in the "Technology and Security" forum of Website X, there is a thread entitled "Information Security and Anti-Forensics" which collects suggestions from multiple users extensively detailing various techniques to avoid and defeat law enforcement detection. This document advises members of Website X to use hidden "TrueCrypt" containers to prevent law enforcement detection of their collection, in the event that the member is caught, explaining "a hidden container (or, a hidden OS), is a hidden, encrypted container that the LEA cannot prove exists. So, you have two keys: a key for the public container and a private container. You can unlock one or

the other at one time, but not both at the same time. So, you can give the LEA the key that opens up your public container whilst hiding the key for your private container. The LEA cannot determine if you have a private, hidden OS, or a private container."

53. Based upon the above information and my training and experience, there is a reasonable probability that the subject under investigation uses encryption software which, if activated, may prevent law enforcement from obtaining the information stored in the computers which are subject to seizure. If, at the time agents enter to execute this search warrant, an encrypted computer is powered off or locked, then the encryption would be activated and it would be difficult or impossible to search that device without the necessary password or pass-phrase. To avoid the scenario where agents encounter an encrypted computer or computers, agents will attempt to execute this warrant at a time when the subject under investigation is home and computers at the subject location are up and running and being used to send or receive data over the Internet. Precautions also need to be taken to ensure that the subject under investigation does not activate encryption when agents arrive at the home to serve the warrant. Activating that encryption can be as simple as pressing a button on a computer or powering a computer down, which takes a matter of seconds. If the subject under investigation or others in the premises is aware of the search prior to the actual entry of the agents who are conducting the search, the encryption software can therefore be easily activated.

54. This has proven to be true investigations similar to the instant investigation on websites operating on the Network dedicated to the advertisement and distribution of child pornography. Prior search warrants obtained by the HSI and other

federal and foreign law enforcement agencies have identified multiple subjects whose computers contained encryption software, including TARGET A and TARGET B, and members of Website X that have been identified. In several of these instances, law enforcement was able to execute the warrants with court-authorized no-knock authority at times when the subjects were at home and the computers at these locations were up and running. This resulted in law enforcement obtaining information leading to multiple identifications and arrests of criminal suspects who were sexually abusing children, producing child pornography, and trafficking in child pornography.

55. For example, during the execution of a search warrant on one administrator of another similar website, the subject attempted to pull his power cables out of the wall to shut down his computer before law enforcement agents took him into custody. The subject did manage to pull a power cable but he missed and grabbed the wrong one. If he had pulled the proper cable his computer would have been shut down and fully encrypted. Because the search team managed to execute the court-authorized no-knock warrant in a timely manner, law enforcement agents seized the subject's computer while it was unencrypted.

56. During the execution of a search warrant on another administrator on a similar website, the subject initiated the process of shutting down his computer and unplugged an encrypted drive before agents took him into custody. Some of his content was still open and decrypted but some was encrypted when he was detained. Because the agents executed the court-authorized no-knock warrant in a timely manner, crucial evidence was obtained and preserved.

57. By contrast, during the execution of a search warrant on another administrator of another target website, the subject was not at his computer when agents entered the residence. His computers were shut down and fully encrypted. That subject's computers were not able to be decrypted by law enforcement without the subject volunteering his password or password.

58. Accordingly, in order to minimize the possibility that agents will encounter encrypted computers, your affiant respectfully requests that this warrant be a "no knock" warrant allowing agents to make a dynamic entry into the residence before announcing their presence, in order to prevent the activation of encryption software, at any time of day or evening at which agents can determine that the subject under investigation is home.

ATTACHMENT A

DESCRIPTION OF LOCATION TO BE SEARCHED

The entire property located at 5412 S. Hately Avenue, Cudahy, Wisconsin 53110, including the residential building, any outbuildings, and any appurtenances thereto (the SUBJECT PREMISES). The SUBJECT PREMISES is located at 5412 S. Hately Avenue, Cudahy, Wisconsin more particularly described as a single story residence, with light brown brick on four sides, and dark brown wood trim covering a majority of the front of the residence. The residence has a front porch area with brown pillars, and the window trim is tan. There is an attached one car garage on the south side of the residence. The outer front door is brown. The numbers "5412" are gold colored and are to the right of the front door entrance. The residence is on the east side of the street, and is the second residence south of East Mallory Avenue.

ATTACHMENT B

ITEMS TO BE SEIZED

The following materials, which constitute evidence of the commission of a criminal offense, contraband, the fruits of crime, or property designed or intended for use or which is or has been used as the means of committing a criminal offense, namely violations of Title 18, United States Code, Sections 2251, 2252 and 2252A:

1. Computers or storage media used as a means to commit the violations described above.
2. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):
    a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;
    b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
    c. evidence of the lack of such malicious software;

d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to the crime(s) under investigation and to the computer user;

e. evidence indicating the computer user's knowledge and/or intent as it relates to the crime(s) under investigation;

f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

g. evidence of programs (and associated data) that are designed to eliminate data from the COMPUTER;

h. evidence of the times the COMPUTER was used;

i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

k. records of or information about Internet Protocol addresses used by the COMPUTER;

l. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses; and

m. contextual information necessary to understand the evidence described in this attachment.

3. Routers, modems, and network equipment used to connect computers to the Internet.

4. Child pornography and child erotica.

5. Any and all images of minors.

6. Records, information, and items relating to violations of the statutes described above including:

    a. Records, information, and items relating to the occupancy or ownership of the SUBJECT PREMISES, 5412 S. Hately Avenue, Cudahy, Wisconsin, including utility and telephone bills, mail envelopes, or addressed correspondence;
    b. Records, information, and items relating to the ownership or use of computer equipment found in the above residence, including sales receipts, bills for Internet access, and handwritten notes;
    c. Records and information relating to the identity or location of the persons suspected of violating the statutes described above;
    d. Records and information relating to the sexual exploitation of children, including correspondence and communications between users of "Website X;"
    e. Records and information showing access to and/or use of "Website X;" and
    f. Records and information relating or pertaining to the identity of the person or persons using or associated with "pantylvr".

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical,

arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded, including external and internal hard drives, flash drives, thumb drives, micro SD cards, macro SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, floppy disks, compact discs, magnetic tapes, memory cards, memory chips, and other magnetic or optical media.

ATTACHMENT A

ITEMS TO BE SEIZED

The following materials, which constitute evidence of the commission of a criminal offense, contraband, the fruits of crime, or property designed or intended for use or which is or has been used as the means of committing a criminal offense, namely violations of Title 18, United States Code, Sections 2251, 2252 and 2252A:

1. Computers or storage media used as a means to commit the violations described above.
2. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):
    a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;
    b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
    c. evidence of the lack of such malicious software;

d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to the crime(s) under investigation and to the computer user;

e. evidence indicating the computer user's knowledge and/or intent as it relates to the crime(s) under investigation;

f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

g. evidence of programs (and associated data) that are designed to eliminate data from the COMPUTER;

h. evidence of the times the COMPUTER was used;

i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

k. records of or information about Internet Protocol addresses used by the COMPUTER;

l. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses; and

m. contextual information necessary to understand the evidence described in this attachment.

3. Routers, modems, and network equipment used to connect computers to the Internet.

4. Child pornography and child erotica.

5. Any and all images of minors.

6. Records, information, and items relating to violations of the statutes described above including:

   a. Records, information, and items relating to the occupancy or ownership of the SUBJECT PREMISES, 5412 S. Hately Avenue, Cudahy, Wisconsin, including utility and telephone bills, mail envelopes, or addressed correspondence;
   b. Records, information, and items relating to the ownership or use of computer equipment found in the above residence, including sales receipts, bills for Internet access, and handwritten notes;
   c. Records and information relating to the identity or location of the persons suspected of violating the statutes described above;
   d. Records and information relating to the sexual exploitation of children, including correspondence and communications between users of "Website X;"
   e. Records and information showing access to and/or use of "Website X;" and
   f. Records and information relating or pertaining to the identity of the person or persons using or associated with "pantylvr".

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical,

arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded, including external and internal hard drives, flash drives, thumb drives, micro SD cards, macro SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, floppy disks, compact discs, magnetic tapes, memory cards, memory chips, and other magnetic or optical media.